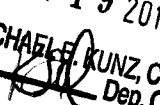


**HB**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

**FILED**  
NOV 19 2012  
MICHAEL E. KUNZ, Clerk  
By  Dep. Clerk

UNITED STATES OF AMERICA,

Plaintiff,

v.

FIRST BANK OF DELAWARE,

Defendant.

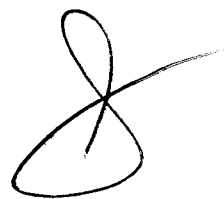
CIVIL ACTION NO.

**12 6500**

**CIVIL COMPLAINT**

Plaintiff, the United States of America, by its attorneys, Zane David Memeger, United States Attorney for the Eastern District of Pennsylvania, and Joel M. Sweet, Susan Dein Bricklin, and Judith A. Amorosa, Assistant United States Attorneys for the same district, alleges as follows:

1. This is a civil action by the United States of America against First Bank of Delaware ("First Bank of Delaware" or the "Bank").
2. From 2009 to 2011, First Bank of Delaware engaged in a scheme to defraud consumers by originating electronic-payment transactions knowing, or by remaining willfully blind to the fact, that the consumer authorizations for the transactions had not been obtained, or had been obtained by dishonest merchants using fraud, trickery, and deceit.
3. First Bank of Delaware originated more than two million debit transactions – worth more than a hundred million dollars – on behalf of third-party payment processors in cahoots with fraudulent Internet and telemarketer merchants, and directly with other fraudulent merchants.



4. First Bank of Delaware was at all relevant times under obligations pursuant to federal statutes and regulations, including but not limited to the Bank Secrecy Act, 31 U.S.C. § 5311 et seq., Section 326 of the USA Patriot Act, 31 U.S.C. § 5318, and regulations including 31 C.F.R. § 103.11 et seq. (2009) (amended 31 C.F.R. § 1020 et seq. (2011)), to know the entities to whom it provided access to the banking system, and to have established procedures to prevent the Bank from providing banking system access to parties engaged in fraud against consumers. First Bank of Delaware ignored and violated these obligations. As a consequence, First Bank of Delaware and the merchants and third-party payment processors for whom First Bank of Delaware originated fraud-tainted transactions caused significant losses to consumers.

## **I. JURISDICTION AND VENUE**

5. This Court has jurisdiction of this action pursuant to 28 U.S.C. § 1331 (federal question) and 28 U.S.C. § 1345 (United States as plaintiff).

6. Venue is proper in the Eastern District of Pennsylvania pursuant to 28 U.S.C. § 1391(b) because defendant First Bank of Delaware operates and maintains its management offices and its operations center in this district, and a substantial part of the events or omissions giving rise to the claims alleged in this complaint occurred in this district. First Bank of Delaware conducts business within this district.

## **II. PARTIES**

7. Plaintiff is the United States of America.

8. Defendant is First Bank of Delaware, a corporation established under the laws of Delaware. First Bank of Delaware's primary location for all business activity is 50 South 16th Street, Philadelphia, PA 19102. This location also is where all of the Bank's senior officers have

primary offices, and where the Bank's operations center is located. First Bank of Delaware also maintains an office at 1000 Rocky Run Parkway, Wilmington, Delaware.

9. As of December, 31 2011, First Bank of Delaware had more than \$200 million in assets and shareholder equity in excess of \$40 million.

10. Initially, the Bank's business model was more closely aligned with a high yielding consumer finance company than with a traditional community bank. The Bank offered a variety of consumer products, including credit and banking services, short-term consumer installment loans, credit and prepaid card products.

11. In or about late 2009, First Bank of Delaware developed an electronic payment program ("E-Payment Program") through which it originated electronic credit and debit transactions on behalf of third-party payment processors and merchants.

12. First Bank of Delaware's Chief Executive Officer at all relevant times hereto was Alonzo J. Primus. At various times Primus also served in additional senior management positions at the Bank.

13. In addition to Primus, officers of the Bank with responsibility for implementation and/or oversight of its E-Payments Program include: Sian Bastable, Vice President and Director of E-Payments Program; Lisa Vandercook, Chief Risk and Compliance Officer; and Daniel Mignogna, Executive Vice President and Chief Operating Officer.

14. During the past several years, the Better Business Bureau's rating for First Bank of Delaware – on a scale of A to F – was an F. The ratings have been based on numerous consumer complaints, particularly concerning billing and collections.

15. First Bank of Delaware has had a troubling history of regulatory actions. On or about October 9, 2008, First Bank of Delaware agreed to the imposition of a Consent Order as a result of adverse findings by the Bank's regulator, the Federal Deposit Insurance Corporation ("FDIC"), concerning the operation of the Bank.

16. On or about December 29, 2011, First Bank of Delaware agreed to another FDIC Consent Order. The FDIC's findings specifically addressed the Bank's origination of electronic payments for third-party payment processors, suspected fraudulent merchants, and money services businesses. The FDIC required First Bank of Delaware to terminate its electronic payments program, including any and all services, products, and/or relationships involving payment processing by or through an automated clearing house, the origination and/or processing of remotely created checks, and/or merchant acquisition.

17. On May 2, 2012, First Bank of Delaware announced publicly its intention to sell its assets to another financial institution and to cease banking operations by the end of 2012. On October 23, 2012, the Bank's shareholders' approved the Bank's dissolution.

### **III. THE FINANCIAL INSTITUTIONS REFORM, RECOVERY AND ENFORCEMENT ACT**

18. The United States seeks civil penalties under the Financial Institutions Reform, Recovery and Enforcement Act, 12 U.S.C. § 1833a ("FIRREA").

19. In 1989, Congress enacted FIRREA as part of a comprehensive legislative plan to reform and strengthen the banking system and the federal deposit insurance system that protects the public from bank failures. Toward that end, FIRREA authorizes civil enforcement of

enumerated criminal predicate offenses – as established by a preponderance of the evidence – that affect financial institutions and certain government agencies.

20. There are several predicate criminal offenses that can form the basis of liability under FIRREA. See 12 U.S.C. § 1833a(c) (Title 18, Sections 215, 656, 657, 1005, 1006, 1007, 1014, 1344; Sections 287, 1001, 1032, 1341, and 1343, affecting a federally insured financial institution; and Title 15, Section 645(a)).

21. The criminal offense relevant to this case is 18 U.S.C. § 1343 – Wire Fraud, affecting a federally-insured financial institution. Section 1343 proscribes the use of a “wire . . . in interstate or foreign commerce” for the purpose of executing, or attempting to execute, “[a] scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises . . . .”

22. The knowledge element of a wire fraud charge can be satisfied with evidence that a defendant “deliberately closed his eyes to what otherwise would have been obvious to him.” United States v. Leahy, 445 F.3d 634, 652 (3d Cir. 2006).

23. FIRREA’s penalty provisions provide that the United States may recover civil penalties (paid to the United States Treasury) of up to \$1 million per violation, or, for a continuing violation, up to \$1 million per day or \$5 million, which ever is less. 12 U.S.C. § 1833a(b)(1)-(2). The statute further provides that the penalty can exceed these limits to permit the United States to recover the amount of any gain to the person committing the violation, or the amount of the loss to a person other than the violator stemming from such conduct, up to the amount of the gain or loss. 12 U.S.C. § 1833a(b)(3).

24. The United States alleges that First Bank of Delaware violated 18 U.S.C. § 1343 affecting a federally-insured financial institution, that the Bank is civilly liable under FIRREA,

and that the United States is entitled to recover as a civil penalty an amount equal to the losses of the consumers victimized by First Bank of Delaware and the third-party payment processors and fraudulent merchants to whom the Bank provided access to consumers' bank accounts.

**IV.  
THE ESSENTIAL ROLE OF BANKS IN  
MASS MARKET CONSUMER FRAUD SCHEMES**

25. Mass market consumer fraud refers to schemes directed at large groups of individuals most often facilitated through the Internet, by telemarketers, and through United States Postal Service mail.

26. Senior citizens are the most common victims of mass market fraud schemes, such as fraudulent telemarketing. According to the AARP, the National Association of Attorneys General, and the Federal Trade Commission, the majority of fraudulent telemarketing victims are age sixty-five or older.

27. Mass market consumer fraud generally involves a scheme that uses deceptive and misleading offers for products and services to induce unsuspecting consumers to provide personal payment information, such as a credit card number or a bank account number.

28. Once in possession of consumers' personal payment information, the scammer – referred to here as the fraudulent merchant – must access the banking system to gain access to the consumer's money.

29. Fraudulent merchants, however, cannot directly access the national banking payment system. To take consumers' money, a fraudulent merchant must establish a relationship with a bank. The bank must agree to originate debit transactions through the national banking system by which money will be withdrawn from consumers' bank accounts and transferred to the fraudulent merchant's bank account.

30. Banks value their reputations and generally do not want to appear to be doing business with fraudulent merchants. For this reason, banks often will not agree to provide access to the national banking system directly to a merchant with a dubious background and suspicious, high risk business practices.

31. To overcome this hurdle and gain access to the national banking system and consumers' accounts, fraudulent merchants often engage third-party payment processors to establish a relationship with a bank. A third-party payment processor serves as an intermediary between the fraudulent merchant and the bank. Through this relationship, a bank can profit from the fees it receives from the third-party payment processor and the fraudulent merchant, while avoiding a direct relationship with the fraudulent merchant and the scrutiny that such a relationship would draw to the bank.

32. A bank is required by law to take steps to enable it to form a reasonable belief that it knows the nature of its clients and their businesses. Mandated Know Your Customer ("KYC") rules are designed to assure that a bank understands the business and character of its clients to whom it is allowing access to the national banking system. Similarly, banks are required to have effective compliance programs to prevent illegal use of the banking system by the bank's clients. See Bank Secrecy Act, 31 U.S.C. § 5311 et seq., and implementing regulations.

33. Banks such as First Bank of Delaware are required to conduct meaningful investigations of new clients at the time of the opening of an account. Before opening a new account for a new client, a bank is required to have in place a Customer Identification Program ("CIP") that is appropriate for its size and type of business, and that includes certain minimum requirements. Banks are required to have a CIP incorporated into the bank's Bank Secrecy

Act/Anti-Money Laundering compliance program. The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each of its customers. A CIP must include account opening procedures that specify identifying information obtained from each customer. A CIP is required to include reasonable and practical risk-based procedures for verifying the identity of each client. See 31 C.F.R. § 103.121 (2009) (amended 31 C.F.R. § 1020.220 (2011))

34. By conducting a meaningful KYC analysis, including an assessment of the client's customer base and product offerings, a bank such as First Bank of Delaware was required to collect information sufficient for the bank to determine whether a client posed a threat of criminal or other improper conduct. See Federal Financial Institutions Examination Council Bank Secrecy/Anti-Money Laundering Examination Manual (2006) at 21 (information required to be collected includes purpose of the account, actual and anticipated activity in the account, the nature of the client's business, the client's location, and the types of products and services the client intended to offer).

35. The banking industry is aware that there is significant risk in originating transactions for third-party processors, particularly where a bank does not have a direct relationship with the merchants for whom it is originating the transactions. The banking industry also knows that fraudulent merchants attempt to frustrate banks' KYC efforts by using third-party payment processors to establish indirect relationships with banks.

36. Federal bank regulators issued additional explicit warnings to the banking industry about the risk of payment processor relationships in 2008, after Wachovia Bank agreed to settle class action litigation and a regulatory action in connection with alleged consumer fraud. Wachovia Bank had originated transactions for several third-party payment processors and

scores of fraudulent telemarketers causing more than \$160 million in consumer losses, resulting in a criminal prosecution of that bank.

37. By the time First Bank of Delaware began to originate electronic transactions for third-party payment processors and fraudulent merchants, the FDIC already had warned banks that third-party payment processors and merchants with high rates of returned transactions may indicate fraud against consumers. The FDIC explained to banks:

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs, which often are evidence of fraudulent activity. High levels of [transactions] returned as unauthorized or due to insufficient funds can be an indication of fraud.

FDIC Guidance of Payment Processor Relationships (FDIC FIL-127-2008) (November 7, 2008).

38. The FDIC further stated that banks should take affirmative steps to assure that they are not abetting consumer fraud by taking additional steps, including the following: (a) monitor all transaction returns (unauthorized returns and total returns); (b) review third-party payment processor promotional materials to determine its target clientele; (c) determine whether the third-party payment processor resells its services to other entities; (d) review the third-party payment processor's policies and procedures to determine adequacy of merchant due diligence; (e) review main lines of business and return volumes for third-party payment processor's merchants; (f) require that the third-party payment processor provide the bank with information about its merchants to enable the bank to assure that the merchant is operating a legitimate business. Id.; see also FDIC Guidance for Managing Third-Party Risk (FIL-44-2008) (June 2008).

39. By the time First Bank of Delaware began to originate electronic transactions for third-party payment processors and fraudulent merchants, the Office of the Comptroller of the

Currency (“OCC”) had warned the banking industry of the risks in providing banking services to third-party payment processors on behalf of telemarketers and other merchant clients. See Payment Processor, Risk Management Guidance (OCC-2008-12) (April 24, 2008). The OCC specifically warned banks to implement a risk management program that included procedures for monitoring processor information such as merchant data, transaction volume, and charge-back history.

40. By the time First Bank of Delaware began to originate electronic transactions for third-party payment processors and fraudulent merchants, the Federal Financial Institutions Examination Council (“FFIEC”) had already for several years been warning the banking industry that third-party payment processors pose a significant risk of consumer fraud. FFIEC, which comprises all of the federal bank regulatory agencies and is empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions, advised:

Banks with third party payment processor customers should be aware of the heightened risk of unauthorized returns and use of services by higher-risk merchants. Some higher-risk merchants routinely use third parties to process their transactions because of the difficulty they have in establishing a direct bank relationship. These entities might include certain mail order and telephone order companies, telemarketing companies, illegal online gambling operations, online payday lenders, businesses that are located offshore, and adult entertainment businesses. Payment processors pose greater money laundering and fraud risk if they do not have an effective means of verifying their merchant clients’ identities and business practices. Risks are heightened when the processor does not perform adequate due diligence on the merchants for which they are originating payments.

Bank Secrecy Act Anti-Money Laundering Examination Manual: Third-Party Payment

Processors – Overview (2010).<sup>1</sup>

**A. ACH Debits and Remotely-Created Checks: Payment Instruments Favored By Third-party Payment Processors and Their Fraudulent Merchants.**

41. Automated Clearing House (“ACH”) debit transactions and remotely-created checks (“RCCs”) are two of the primary transaction instruments used by mass market fraudulent merchants to take money from consumers’ bank accounts.

42. ACH is an electronic network for financial transactions in the United States. ACH processes large volumes of transactions, both credits into accounts and debits out of accounts, for merchants. The rules and regulations governing the ACH network are established by NACHA (formerly the National Automated Clearing House Association) and the Federal Reserve.

---

<sup>1</sup> At the time First Bank of Delaware originated fraud-tainted transactions on behalf of third-party payment processors and merchants, regulatory guidance to banks was clear and unambiguous. Since then, regulators have reemphasized past guidance. For example, the FDIC issued “Payment Processor Relationships – Revised Guidance” (FIL-3-2012) (January 31, 2012) (*“Financial institutions that fail to adequately manage [third-party payment processor] relationships may be viewed as facilitating a payment processor’s or merchant client’s fraudulent or unlawful activity and, thus, may be liable for such acts or practices”* (italics in original); see also “Managing Risks in Third-Party Payment Processor Relationships,” FDIC Supervisory Insights Journal (Summer 2011).

Similarly, the Financial Crimes Enforcement Network of the Department of the Treasury (“FinCEN”), which is charged with protecting the nation’s financial system from money laundering and terrorist financing, recently issued an Advisory that further emphasized the risks arising from bank relationships with third-party payment processors. The Advisory highlights the need for banks to conduct due diligence of processors and their merchants, to pay close attention to return and chargeback rates, and the need for banks to assure that processors have obtained all necessary state licenses, registrations, and approvals. See “Risk Associated with Third-Party Payment Processors,” (FIN-2012-A010) (October 22, 2012), [www.fincen.gov/statutes\\_regs/guidance/html/FIN-2012-A010.html](http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A010.html).

43. An RCC is a check created not by the account holder but rather by a third-party using the account holder's name and bank account information.<sup>2</sup> Unlike ordinary checks, RCCs are not signed by the account holder. In place of the account holder's signature, an RCC contains a statement claiming that the customer has authorized the check. Often an RCC will have a legend stating something similar to "Authorized By Your Depositor No Signature Required Reference # XXXXXX."

44. RCCs are notorious in the banking industry and in the consumer protection community as instruments of fraud. In a 2005 letter to the Board of Governors of the Federal Reserve System, the Attorneys General of 35 states jointly urged that RCCs be eliminated from the banking system. The Attorneys General explained that RCCs are "used to perpetrate fraud on consumers" by causing the withdrawal of money from consumers' bank accounts without authorization.

45. From 2009 to 2011, First Bank of Delaware originated more than \$138 million in RCC transactions on behalf of merchants and third-party payment processors.

46. To execute valid ACH and RCC debit transactions, an initiating merchant must provide to its own bank: (1) a consumer's bank routing number; (2) a consumer's bank account number; and (3) proof that the consumer authorized the transaction.

47. This case concerns First Bank of Delaware's knowledge – or willful blindness to the fact – that the ACH debit and RCC transactions that it originated for its merchants and third-party processors were not based on consumer authorizations, but instead were based on fraud.

---

<sup>2</sup> RCC's also are referred to as "demand drafts," "preauthorized drafts," "electronic RCCs," "electronic payment orders, remotely-created payment orders," "electronic checks," and "check 21 e-checks."

**B. High Return or Chargeback Rates Are a Red Flag That A Bank's Client Merchant Is Defrauding Consumers.**

48. A rejected ACH debit or RCC transaction is referred to in the banking industry as a "return" or a "chargeback." A return or chargeback reflects a transaction that was rejected by the consumer or the consumer's bank and was thus not successful in taking funds from the account of the consumer. A return "rate" refers to number of returned items compared to the number of originated transactions during a particular time period.

49. High return rates are not absolute proof of fraud; rather, they are a red flag that a merchant's practices may be deceptive or otherwise dishonest. High return rates trigger a duty by the bank and the third-party payment processor to inquire into the reasons for the high rate of returns, and specifically whether the merchant is engaged in fraud.

50. ACH debits and RCCs may be rejected for a number of reasons, including lack of authorization by the consumer, insufficient funds in the consumer's account, or a closed account. "Unauthorized" returns expressly reflect a consumer having denied that he or she authorized a transaction. Other stated return reasons similarly reflect unauthorized or suspicious transactions requiring inquiry and investigation. For example, returned RCCs stamped "Refer to Maker" are widely known in the banking industry to reflect inadequate consumer authorization or to be otherwise suspicious. Likewise, high rates of returns for reasons such as "closed account" can reasonably suggest that consumers were forced to close their bank accounts to protect themselves from further unauthorized withdrawals. High rates of returns for "insufficient funds" may be evidence that prior unauthorized withdrawals have depleted a consumer's bank account. Accordingly, high rates of total returns (as opposed to only unauthorized returns) may indicate potential fraud and must trigger inquiry.

51. ACH debit transaction return rates are relatively easy to monitor electronically because the transactions are processed through the clearing houses. Under the applicable NACHA rules, a bank or a merchant must take corrective action where a merchant's unauthorized return transaction rate for ACH debits exceeds 1 percent.

52. RCCs returned transactions are not monitored electronically and there is no threshold for corrective action. Banks therefore must analyze return transaction rates for the RCCs that it submits into the national banking system, and consider the returned transaction rate in the context of the fact that the return rate for all checks transacted through the national banking system is only one half of one percent (.5 percent).

**V.**

**FIRST BANK OF DELAWARE ENGAGED IN WIRE FRAUD BY  
PROCESSING RCC AND ACH TRANSACTIONS THAT IT  
KNEW WERE BASED ON FRAUD AGAINST CONSUMERS**

53. Many banks heeded the guidance of federal bank regulators and law enforcement and scrutinized their relationships with third-party payment processors and high-risk merchants to protect consumers from fraud and to protect themselves from reputational, regulatory, and legal risk.

54. First Bank of Delaware was not one of those banks. On the contrary, First Bank of Delaware recognized that enormous profits could be reaped by originating electronic transactions on behalf of fraudulent merchants directly and through third-party payment processors. For First Bank of Delaware, the potential profits outweighed the fraud risk to consumers.

55. First Bank of Delaware engaged in wire fraud by processing RCC and ACH transactions that it knew were based on fraud against consumers, or by remaining willfully blind to that fact. This was not surprising in light of the Bank's history.

56. First Bank of Delaware's business practices have become the subject of law enforcement and consumer protection agencies' actions for years. For example, on April 26, 2007, the State of California filed an action against First Bank of Delaware alleging that First Bank of Delaware and others engaged in unlawful and deceptive business practices to avoid California laws regulating the provision of payday loans and other types of short-term consumer loans to California customers. See The People of the State of California v. Check 'N Go of California, Inc., et al., Superior Court of California, County of San Francisco, Civil Action No. 07-462779.

57. On or about June 10, 2008, the FDIC initiated an enforcement action against First Bank of Delaware and other financial institutions in connection with the marketing of sub-prime credit cards in violation of the Federal Trade Commission Act. The FDIC and the State Bank Commissioner of Delaware found deficiencies in the Bank's management, board participation, strategic planning, oversight of third parties, and compliance management system and audit program. As previously alleged, in a Consent Order dated on or about October 9, 2008, First Bank of Delaware was required to terminate third-party lending programs and to substantially increase its board of directors and management oversight of its business. The FDIC also required First Bank of Delaware to establish an account in the amount of \$700,000 to ensure the availability of restitution to its consumer victims, and to pay a \$304,000 civil money penalty to the United States Treasury.

58. Forced to end lucrative predatory activities, First Bank of Delaware looked to develop alternative revenue streams that would provide high financial returns, and considered businesses such as electronic payment services, prepaid credit cards, and check cashing operations.

59. By June 2009, First Bank of Delaware had decided to develop what it called an “E-Payments Program” that it anticipated would generate fee income from the origination of electronic payments. The E-Payments Program would have three primary components: (1) originating RCC transactions; (2) originating ACH transactions; and (3) credit card merchant acquisition.

60. First Bank of Delaware recognized that the E-Payments Program business model would involve high risk to the Bank. The Bank specifically knew that it would be providing RCC transaction services to high risk Internet merchants. In fact, Chief Executive Officer Primus and Chief Risk and Compliance Officer Vandercook repeatedly informed the Bank’s Board of Directors that the Bank would have a “robust oversight process” to protect against that risk. The oversight process was to include due diligence of third-party payment processors and merchants, monitoring of the “volume of net returns” of transactions, and a variety of other regular monitoring practices. Primus also announced the creation of an E-Payments Program Risk Committee, which he said would be comprised of officers of the Bank.

61. In 2010, First Bank of Delaware agreed to originate debit transactions for third-party payment processors Landmark Clearing, Inc. (“Landmark Clearing”), Automated Electronic Checking, Inc. (“AEC”), Check Site, Inc. (“Check Site”), and Check 21.com, LLC (“Check 21”). The Bank’s Board of Directors had been informed that Vandercook was deeply involved in the due diligence investigations of these four third-party payment processors.

62. In recognition of the risk, the Bank included numerous provisions in its contracts with the third-party processors addressing return rates for RCCs. The contracts included provisions that if any of the merchant returns of “unauthorized,” “fraud,” or any other category of “unauthorized” return exceeded one (1) percent of originated volumes, at the sole discretion of the Bank, the Bank could retain money in the processor’s reserve accounts. Further, unauthorized return activity above certain thresholds could result in termination and/or suspension of RCC processing, in the Bank’s sole discretion.

63. By May 10, 2010, according to Board of Director Meeting minutes, the Bank had developed a strategy to grow its E-Payments Program. First Bank of Delaware anticipated that its revenue from its E-Payments Program would grow from \$150,000 in 2010 to \$2,000,000 in 2011 – an increase of more than 1,300 percent.

64. By this time, however, the Bank already knew that its E-Payment Program was under the scrutiny of regulators because its return transaction rate was extremely high, and that the high return rates indicated that the Bank was originating fraud-tainted transactions. In May 2010, a Federal Reserve official wrote to First Bank of Delaware stating:

[A] return rate of 10% (which is on its face significantly in excess of industry norms) would likely be regarded by bank supervisory agencies and/or law enforcement agencies as prima facie evidence that your bank knew or should have known that your [third-party payment processors and/or merchants] had engaged in fraudulent activities. Whether a return rate of 10% might expose your bank to potential liability is an issue that we urge you to consider carefully in consultation with your legal counsel.

65. In August 2010, First Bank of Delaware originated more than \$4.9 million in debit transactions for Landmark Clearing, more than \$7 million in debit transactions for Check

Site, and more than \$1.2 million in debit transactions for Check 21. First Bank of Delaware also originated more than \$1.5 million in transactions for a merchant known as Monster Rewards.

66. First Bank of Delaware recognized that high return rates on RCC transactions were a red flag warning of risk to the Bank. Primus informed the Bank's Board of Directors in August 2010 that the Bank would perform "high level monitoring of any merchant" with an unauthorized return rate of 2 percent or more, and that a risk committee would review merchants with high return rates, as well as "monitor return reasons, customer calls and any complaints to determine whether merchants should be terminated."

67. By October 2010, Executive Vice President and Chief Operating Officer Mignogna informed the Bank's Board of Directors that ACH transaction volume had reached \$100 million per month, and that RCC volume had reached \$10 million per month. Mignogna further stated that the Bank had terminated merchants for high unauthorized return rates and complaints, and that the Bank was "constantly monitoring return and chargeback rates to ensure we manage risk in the portfolio."

68. Despite the Bank officers' assurances to the Board of Directors regarding the Bank's purported robust compliance plan, third-party payment processors Landmark Clearing, Check Site, Check 21, and AEC had aggregate return rates on RCC transactions exceeding 50 percent. Indeed, often the return rates were significantly higher than 50 percent. By comparing a single month's originated transactions to the same month's returned items to achieve a return rate, in December 2010 AEC processing for ZaZaPay had a return rate of 81 percent. In the same month Landmark Clearing processing for Platinum Online Group had a return rate of 84 percent. In September 2010, Check 21 processing for Complete Family Coverage had a return

rate of 84 percent. And in August 2010, Check Site processing for Belfort Capital Ventures had a return rate of 57 percent.

69. For one or more months between April 2010 and March 2011, the same third-party payment processors also had unauthorized return rates well above two percent for some of their merchants – exceeding the Bank’s stated threshold for merchant termination. For example, in June, July and August, 2010, Check 21’s merchant Web Savers had unauthorized return rates of 7.28 percent, 6.36 percent, and 10.24 percent, respectively, yet the Bank did not terminate Web Savers in accordance with its stated policy.

70. On January 14, 2011, the Bank’s Board of Directors learned at an FDIC exit interview that the FDIC had grave concerns about the Bank’s E-Payments Program. The Board of Directors ordered the Bank’s officers to disclose additional facts about the E-Payments Program. The Board of Directors thereafter concluded that the Bank’s underwriting of its merchants and third-party payment processors had not been adequate, that certain merchants experienced very high return rates, and – in an extraordinary example of understatement – that some merchants “offer products whose value to the consumer could be questioned.”

71. In January 2011, Primus informed the Board of Directors that by February 28, 2011, the Bank would terminate certain high risk merchants that represented 90 percent of the Bank’s RCC transaction volume. In fact, the Bank did not terminate most of the fraudulent merchants until late-Spring 2011.

72. The remaining components of the Bank’s E-Payments Program – ACH debit transactions and merchant acquiring – also experienced similar problems. A review of First Bank of Delaware’s merchant acquiring program conducted in January 2011 revealed significant material failures by the Bank in conducting due diligence and monitoring. As a result of the

Bank's relationship with merchant LeanSpa, LLC, which markets a supposed weight-loss supplement, the Bank was required to pay VISA more than \$1.8 million in chargeback fees. First Bank of Delaware finally terminated LeanSpa in April 2011 due to excessive chargebacks.

73. First Bank of Delaware provided banking services to at least four third-party payment processors, each of which provided services to a substantial number of merchants with extremely high return rates on consumer transactions. First Bank of Delaware earned a substantial profit from these relationships. For third-party payment processor Landmark, First Bank of Delaware earned a fee of \$1.00 for each returned transaction, and \$2.00 for each return transaction identified as unauthorized. The higher fee for returned transaction identified as unauthorized recognized the greater risk to the Bank associated with initiating transactions for merchants engaged in fraud.

74. First Bank of Delaware processed RCCs for these third-party payment processors despite red flags warning that the consumer authorizations supporting the transactions were not genuine, or were induced through fraud. These red flags include (but are not limited to) the high aggregate return rates experienced by these processors for their RCC transactions – a plain indication that the merchants were not honest with consumers.

75. First Bank of Delaware knew that:

a. Landmark Clearing initiated more than 950,000 RCC transactions for an aggregate dollar amount of more than \$57.2 million during the time period April 2010 to March 2011. The aggregate return rate for these transactions was more than 53 percent on a transaction basis, and more than 60 percent on a dollar basis.

b. Check Site initiated more than 1.2 million RCC transactions for an aggregate dollar amount of more than \$46.7 million during the time period May 2010 to March

2011. The aggregate return rate for these transactions was more than 55 percent on a transaction basis, and more than 42 percent on a dollar basis.

c. Check 21 initiated more than 353,000 RCC transactions for an aggregate dollar amount of more than \$15.4 million during the time period April 2010 to March 2011. The aggregate return rate for these transactions was more than 55 percent on a transaction basis, and more than 56 percent on a dollar basis.

d. AEC initiated more than 126,000 RCC transactions for an aggregate dollar amount of more than \$4.2 million during the time period September 2010 to March 2011. The aggregate return rate for these transactions was more than 55 percent on a transaction basis, and more than 59 percent on a dollar basis.

76. These return rates are significant in that they reveal that more than half of the withdrawal transactions that First Bank of Delaware originated on behalf of third-party payment processors were rejected by consumers or by consumers' banks.

77. The government alleges that the Bank – through its officers Primus, Vandercook, Bastable and Mignogna – knew that the merchants for whom First Bank of Delaware processed transactions were engaged in consumer fraud.

78. First Bank of Delaware created internal policies, and included contract provisions in its agreements with third-party processors and merchants, that required due diligence and monitoring of high return rates. Rather than implement these policies and provisions – which would have required the termination of merchant processing and the loss of revenue for First Bank of Delaware – First Bank of Delaware consciously ignored its own policies.

79. First Bank of Delaware failed to conduct due diligence, and it ignored extraordinarily high return rates, so that it could continue to provide banking services for

obviously fraudulent merchants and their accomplice third-party payment processors. First Bank of Delaware ignored information that plainly revealed that merchants or third-party payment processors were engaged in fraud.

**VI.  
FIRST BANK OF DELAWARE ENGAGED IN WIRE FRAUD AGAINST  
CONSUMERS WITH A LARGE NUMBER OF THIRD-PARTY PAYMENT  
PROCESSORS AND MERCHANTS**

80. First Bank of Delaware processed payments for at least four third-party payment processors and more than 40 merchant clients. Following is merely a sample of the third-party payment processors and merchants with whom First Bank of Delaware engaged in wire fraud against consumers.

**A. Landmark Clearing**

81. First Bank of Delaware engaged in wire fraud by providing third-party payment processor Landmark Clearing and its fraudulent merchants access to the national banking system to further a scheme to take money illegally from consumers' accounts.

82. On or about January 6, 2010, First Bank of Delaware entered into a written agreement with third-party payment processor Landmark Clearing of 5340 Legacy Drive, Plano, Texas. The agreement provided that First Bank of Delaware would process RCC transactions for Landmark Clearing and its merchant clients.

83. Landmark Clearing agreed to pay First Bank of Delaware 25 cents for each credit or debit transaction, \$2 for each unauthorized return, and \$1 for each other return.

84. Disregarding its obligation to conduct due diligence on merchants for whom it is providing access to the national banking system, First Bank of Delaware abdicated virtually all of its responsibilities to Landmark Clearing, agreeing that Landmark Clearing would have

“primary responsibilities with respect to the granting, extension or continuance of service to any [m]erchant” for whom First Bank of Delaware would originate RCC transactions.

85. On December 15, 2011, the FTC filed a complaint against third-party payment processor Landmark Clearing and its officers Larry Wubben and Eric Loehr. The FTC alleged that “since at least November 2008” (which includes the time period when the Bank was originating RCC transactions for Landmark Clearing) Landmark debited consumer bank accounts on behalf of its merchants, despite substantial evidence that consumers had not authorized debits to their bank accounts. Landmark Clearing consented to a permanent injunction. See FTC v. Landmark Clearing, Inc., et al., Civil Action No. 4:11-CV-00826 (E.D. Tex.).

86. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and Landmark Clearing to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

**B. Direct Benefits Group**

87. First Bank of Delaware engaged in wire fraud by providing merchant Direct Benefits Group access to the national banking system to further a scheme to take money illegally from consumers’ accounts.

88. Direct Benefits Group was a merchant of Landmark Clearing and Check 21. Direct Benefits purported to offer consumers a discount program for savings on a variety of consumer goods and services.

89. During 2010 and 2011, First Bank of Delaware originated more than \$11.9 million in RCC transactions (more than 254,000 transactions) on behalf of Direct Benefits

Group. In many months during this period, the return rate for Direct Benefits transactions was over 60 percent.

90. First Bank of Delaware was aware that Direct Benefits was cheating consumers, or it remained willfully blind to that fact. The owner of Direct Benefits, Kyle Wood, was an officer of a company, City West Advantage, Inc., that had previously been the subject of a 2008 FTC complaint alleging violations related to deceptive telemarketing sales calls and the unauthorized use of RCCs. City West Advantage was the subject of a July 2009 final judgment and order for permanent injunction in a case brought by the FTC. First Bank of Delaware had a duty to know these facts before providing Direct Benefits Group access to the national banking system and consumers' bank accounts.

91. First Bank of Delaware continued to process for Direct Benefits Group until at least March 2011.

92. On August 19, 2011, the FTC obtained a federal court preliminary injunction against Direct Benefits Group, LLC, its owner Kyle Wood, and other defendants. The FTC had alleged that "since at least September 2009" – which includes the period when the Bank was originating RCC transactions for Direct Benefits Group – Direct Benefits Group debited consumers' bank accounts without their knowledge or consent after Direct Benefits Group had collected financial information from consumers who were seeking payday loans. The court found that Direct Benefits Group had engaged in misleading and deceptive conduct against consumers and therefore entered asset restraints and appointed a permanent receiver. See FTC v. Direct Benefits Group, LLC, et al., Civil Action No. 6:11-CV-01186 (M.D. Fla.).

93. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and Landmark Clearing

and/or Direct Benefits Group to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

**C. The ZaaZoom Companies and their Processors**

94. First Bank of Delaware engaged in wire fraud by providing merchants ZaaZoom Solutions (“ZaaZoom”) and ZaZaPay access to the national banking system to further a scheme to take money illegally from consumers’ accounts.

95. Between May 2010 and March 2011, First Bank of Delaware processed electronic RCC payments for ZazaPay, a company purporting to offer various online marketing services. First Bank of Delaware processed for ZazaPay through several payment processors, including AEC and a chain of two third-party payment processors – the transactions were processed through two payment processors, including Check Site.

96. Despite the already high return rates generated by ZazaPay through these two payment processors, First Bank of Delaware then agreed to simultaneously process electronic RCC payments for ZaaZoom Solutions, a company related to ZazaPay, through yet another payment processor, Landmark. First Bank of Delaware provided banking services to ZaaZoom Solutions despite knowing that it was under scrutiny for potential unfair and deceptive trade practices.

97. ZaaZoom Solutions was a merchant of Landmark Clearing. ZaaZoom purported to offer online advertising services. First Bank of Delaware began to originate RCC transactions for ZaaZoom in April 2010. During an eleven month period, the Bank originated more than \$14.8 million in RCC transactions (more than 460,000 transactions) on behalf of ZaaZoom. The return rate for ZaaZoom transactions was over 51 percent. First Bank of Delaware continued to originate RCC transactions for ZaaZoom until at least February, 2011.

98. Consumer plaintiffs in a class action lawsuit filed in 2011 allege that Zaazoom lured victims into applying for payday loans on internet websites and, in cahoots with First Bank of Delaware, used the applicants' personal banking information to take money from their accounts without authorization. See Marsh v. Zaazoom Solutions, LLC., et al., Civil Action No. 11-5226(N.D. Cal.).

99. First Bank of Delaware monthly generated reports that indicated ZaZaPay's return rate for the transactions it processed from September 2010 through February 2011. During that time the reports indicated that for the transactions processed through AEC the unauthorized return rate ranged from less than 1 percent for the first month to 4.3 percent. The overall return rate was approximately 56 percent. ZaZaPay also processed through Checksite from May 2010 through February 2011. With Checksite their unauthorized return rate ranged from less than 1 percent during the first month to 6.72 percent. Their total return rate for the transactions processed through Checksite was approximately 57 percent. Despite its own policies and procedures, First Bank of Delaware did not stop providing ZaZaPay access to the banking system until after February 2011.

100. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and third-party payment processors Landmark, AEC and Check Site, and/or their merchants Zaazoom and ZaZaPay, to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

**D. Membership Services, d/b/a Monster Rewards**

101. First Bank of Delaware engaged in wire fraud by providing merchant Membership Services, d/b/a Monster Rewards, access to the national banking system to further a scheme to take money illegally from consumers' accounts.

102. First Bank of Delaware provided ACH and RCC transactions on behalf of Monster Rewards. Early in 2010, NACHA informed First Bank of Delaware that Monster Rewards exceeded applicable thresholds for ACH unauthorized returns.

103. In response, in April 2010, First Bank of Delaware intentionally transitioned Monster Rewards from the ACH payment system – where it was under NACHA scrutiny – to an RCC payment platform, where it would be policed – if at all – only by First Bank of Delaware itself. During the following eleven months, First Bank of Delaware processed more than \$14.1 million in RCC transactions (approximately 226,310 transactions) for Monster Rewards. Of that amount, approximately \$9.6 million (approximately 161,024 transactions) was returned, for a return rate of more than 71 percent.

104. Moreover, First Bank of Delaware provided Monster Rewards access to consumers' bank accounts knowing that the FTC had brought an action against the owners of Monster Rewards, and that the FTC had obtained a federal court permanent injunction against the owners of Monster Rewards.

105. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and Monster Rewards and its agents to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

**E. Check 21**

106. First Bank of Delaware engaged in wire fraud by providing third-party payment processor Check 21, and some of its merchants, access to the national banking system to further a scheme to take money illegally from consumers' accounts.

107. Check 21 processed payments through First Bank of Delaware for merchant Web Savers. Web Savers had an unauthorized return rate exceeding 5 percent for five consecutive months from June to October 2010. Similarly, Check 21 merchant Super Club Savings had an unauthorized return rate exceeding 5 percent for six consecutive months from September 2010 to February 2011.

108. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and third-party payment processor Check 21 to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

**F. LeanSpa, LLC**

109. First Bank of Delaware engaged in wire fraud by providing merchant LeanSpa, LLC, access to the national banking system to further a scheme to take money illegally from consumers' accounts.

110. On or about November 14, 2011, the FTC and the State of Connecticut obtained an ex parte restraining order against LeanSpa, LLC, an entity marketing and selling purported weight-loss and colon cleanse products, its owner Boris Mizhen, and other related defendants. In a complaint, the FTC and Connecticut alleged that from "at least September 2010" – which included the period when the Bank was processing Lean Spa's transactions – Lean Spa used deceptive practices to lure consumers to their websites, used deceptive trial offers to induce

consumers to provide credit or debit card information, automatically enrolled consumers in continuity plans where consumers were charged every month and made it difficult for the consumers to cancel these recurring monthly shipments and receive refunds. See FTC and State of Connecticut v. LeanSpa, LLC, Civil Action No. 3:11-CV-1715 (D. Conn.). First Bank of Delaware was processing up to \$1 million per month for LeanSpa by October 2010. In November 2010, First Bank of Delaware agreed to increase LeanSpa's transaction volume to \$1.75 million in transaction payments per month. One month later, in December 2010, the Bank again increased LeanSpa's permissible volume to \$5 million per month.

111. First Bank of Delaware used the Internet and telephones to communicate across state lines for the purpose of transferring information between itself and LeanSpa to further their common scheme to defraud consumers, and to conspire to obtain money by means of false or fraudulent pretenses, representations, or promises.

#### **G. Other Fraudulent Merchants**

112. First Bank of Delaware provided banking system access to Michael Moneymaker and Daniel DeLaCruz and their related companies. On March 28, 2011, the FTC charged Moneymaker and DeLaCruz and their four companies – including Belfort Capital Ventures and Dynamic Online Solutions – with unfairly and deceptively billing consumers without their consent and not providing promised refunds in violation of federal law. Specifically, the FTC charged that “since at least August 2009” – which includes the period during which the Bank processed their transactions – the defendants in that case used personal information obtained from consumers as part of payday loan applications to create RCCs in a scheme to charge recurring fees to consumers without the consumers' authorization. See FTC v. Michael Bruce Moneymaker, et al., Civil Action No. 2:11-CV-00461 (D. Nev.). The defendants in that case

acknowledged they “acquired consumers’ bank account information when those consumers applied for payday loans online and then, without consumers’ consent, debited their bank accounts.” Id., Stipulated Order for Injunction and Monetary Judgment, at ¶ 5.

113. Starting in 2010, First Bank of Delaware processed payment for Belfort Capital Ventures and Dynamic Online Solutions – two of the companies charged in the FTC’s complaint. It processed for both these companies through the third-party processor Check Site, and both of these companies had extraordinarily high returns.

114. Consumer losses arising from the conduct alleged above exceeded \$15 million.

**FIRST CAUSE OF ACTION  
FOR CIVIL PENALTIES UNDER FIRREA**

115. The government incorporates by reference paragraphs 1 through 114 as if fully set forth in this paragraph.

116. By virtue of the conduct described above, and for the purpose of profiting from fees generated for itself by that conduct, First Bank of Delaware unlawfully engaged in a scheme and artifice to defraud consumers, using interstate mail carriers and interstate wire, in violation of the wire fraud statute, 18 U.S.C. § 1343. First Bank of Delaware knew of the criminal conduct described herein, or remained willfully blind to the criminal conduct.

117. This scheme to defraud has affected numerous federally insured financial institutions, including the banks of the consumer victims from whom money was taken without authorization.

118. Accordingly, First Bank of Delaware is liable to the United States for civil penalties as authorized under 12 U.S.C. § 1833a(b).


**WHEREFORE**, the United States requests judgment against defendant First Bank of Delaware, as follows:

- a. A judgment imposing a civil penalty against First Bank of Delaware up to the maximum amount allowed by law;
- b. Such further relief as the Court deems just.

Respectfully,



ZANE DAVID MEMEGER  
United States Attorney




MARGARET L. HUTCHINSON  
Assistant United States Attorney  
Chief, Civil Division



JOEL M. SWEET  
Assistant United States Attorney



SUSAN DEIN BRICKLIN  
Assistant United States Attorney



JUDITH A. AMOROSA  
Assistant United States Attorney  
Office of the United States Attorney  
615 Chestnut Street, Suite 1250  
Philadelphia, PA 19106  
Tel. 215-861-8200  
Fax. 215-861-8618

Dated: November 19, 2012